**Project Initialization and Planning Phase**

|  |  |
| --- | --- |
| Date | 6/18/2025 |
| Team ID | SWTID1749841176 |
| Project Title | Online Payments Fraud Detection using Machine Learning |
| Maximum Marks | 3 Marks |

**Project Proposal (Proposed Solution) report:**

To address the challenges of online fraud and improve the accuracy of detection systems, we propose developing a machine learning-based fraud detection model that analyses real-time transaction data to identify suspicious patterns. The system will leverage supervised learning algorithms trained on historical transaction datasets to classify activities as fraudulent or legitimate. Key features such as transaction amount, location, time, device type, and user behaviour will be used to train the model. The proposed solution aims to reduce false positives, minimize unnecessary user interruptions, and enhance overall transaction security by continuously learning and adapting to new fraud techniques.

|  |  |  |
| --- | --- | --- |
| **Project Overview** | | |
| **Objective** | |  | | --- | |  |  |  | | --- | | To build a machine learning model that accurately detects fraudulent transactions while minimizing false positives and user disruption. | | |
| **Scope** | |  | | --- | |  |  |  | | --- | | The system will focus on detecting fraud in online transactions such as digital banking, e-commerce payments, and wallet services. It will process structured transactional data for fraud classification. | | |
| |  | | --- | | **Problem Statement** |  |  | | --- | |  | | | |
| |  | | --- | | **Description** |  |  | | --- | |  | | | The project involves collecting and preprocessing transaction data, selecting relevant features, and applying ML algorithms (e.g., Logistic Regression, Random Forest, XGBoost) to build a fraud detection model. |
| **Impact** | | |  | | --- | |  |  |  | | --- | | Reduces false alarms, improves user trust, ensures seamless digital transactions, and strengthens the organization’s fraud prevention capabilities. | |
| |  | | --- | | **Proposed Solution** |  |  | | --- | |  | | | |
| **Approach** | | |  | | --- | | Use supervised learning techniques on labelled datasets, evaluate multiple models, perform feature engineering, and deploy the best-performing model with a feedback loop for continuous improvement. |  |  | | --- | |  | |
| |  | | --- | | **Key Features** |  |  | | --- | |  | | | Real-time fraud detection, adaptive learning, minimal false positives, behavioural pattern analysis, dashboard for flagged transactions. |

**Resource Requirements**

|  |  |  |
| --- | --- | --- |
| **Resource Type** | **Description** | **Specification** |
| **Hardware** | | |
| **Computing Resources** | CPU/GPU specification, number of cores | 8 core CPU/GPU |
| **Memory** | RAM specification | 16 GB |
| **Storage** | Disk space for data, models, logs | 100 GB SSD |
| **Software** | | |
| **Frameworks** | Python frameworks | Flask |
| **Libraries** | Additional Libraries | pandas, numpy, matplotlib, seaborn, sklearn, xgboost |
| **Development Environment** | IDE | Jupyter Notebook, VS Code with Python 3.8+ |
| **Data** | | |
| **Data** | Source, Size, Format | Online Payments Fraud Detection Dataset (Kaggle) |